UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,521	06/06/2000	Upendra V. Chaudhari	YOR9-2000-0093US1(8728-35	8243

46069 7590 02/11/2005

F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/588,521	CHAUDHARI ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1 and 12 have been considered but are moot in view of the new grounds of rejection.

The applicant is correct in their characterization of the teachings of Kanevsky that it is not disclosed "the score is used to determine a level of secured data that can be accessed by the user." Based upon the applicant's amendment, further searching and consideration has been conducted wherein the teachings of Fritch has been applied to independent claims 1 and 12.

2. Applicant's arguments filed May 10, 2005 have been fully considered but they are not persuasive.

As per independent claims 1 and 12, the teachings of Kanevsky have been addressed by the applicant as not disclosing "the score is used to determine a level of secured data that can be accessed by the user." It is further argued that it is not taught by the combination of applied references "computing a confidence score based on the identity claim using speech input from the user, wherein the confidence score is a measure of confidence in the validity of the identity claim, and if the confidence score meets a threshold value, providing the user access to secured data having varying levels of security, wherein providing access comprises determining a level of secured data that may be accessed by the user based on the computed confidence score." The applicant asserts that the teachings of Fritch disclose different security levels to data

and access to different levels of security are based on matching the security level of the data to the security level that is assigned to the identity of that particular person that is seeking access to the data as is recited in column 6, lines 18-20 and column 8, lines 18-20. The examiner agrees with the applicant's assertion concerning the teachings of Fritch, however it is noted that the teachings of Fritch are not relied upon solely for "using a measure of confidence of the validity of a person making an identification claims to control access to secured data at different security levels." It is the combination of the teachings of Kanevsky and Fritch that are relied upon for meeting the applicant's claim limitations. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

As per independent claim 23, it is argued by the applicant that the combination of Kanevsky and Fritch fail to disclose "a computation module that computes a confidence score that is a measure of confidence in the validity of an original identity claim provided at a commencement of a dialog session, and a dialog manager for controlling access to data in the database, wherein access to the data classes is limited to a data class in which a last computed confidence score meets or exceeds a confidence score assigned to that data class." It is the combination of the teachings of Kanevsky and Fritch that are relied upon for meeting the applicant's claim limitations.

It is additionally argued for independent claim 23 by the applicant further asserts that Fritch fails to disclose or suggest "classification levels assigned to information objects that are based on confidence measures for the validity of identity claims of a user." In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., classification levels assigned to information objects) are not recited in the rejected claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). It is the combination of the teachings of Kanevsky and Fritch that are relied upon for meeting the applicant's claim limitations. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contains subject matter which was not described in the specification in such a way as to reasonably convey to

one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. The applicant has amended the claims to recite "if the confidence score meets a threshold value" as per independent claims 1 and 12. In regards to Figure 2, the confidence score is computed (item 205) and it is determined if the confidence score is above a predefined threshold (item 206) wherein it is additionally recited in the applicant's specification page 23, line 17 through page 24, line 12. There is no recitation of the confidence score "meeting" a threshold, rather the confidence score either "does not exceed" or "exceeds" the predetermined threshold as is recited in that particular section of the applicant's specification.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-8,12-19, and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky et al, U.S. Patent 5,897,616 in view of Fritch et al, U.S. Patent 6,105,132.

As per claim 1, it is disclosed by Kanevsky et al of a method and software (program) used by hardware (storage device, readable by a machine, tangibly embodying a program of instructions executable by the machine) to perform the authentication a user in a conversational system (col. 1, lines 15-19, col. 5, lines 49-54).

An identity claim is received from a user wherein the first spoken utterances of the speaker are received and the first spoken utterances containing indicia of the speaker (col. 3, lines 23-25). A confidence score is computed based on the identity claim using speech input from the user, wherein the confidence score is a measure of confidence in the validity of the identity claim (col. 3, lines 41-43). If the score matches a threshold value, the user is provided access to secured data based on the computed confidence score (col. 3, lines 44-48 and as recited in the abstract). The teachings of Kanevsky et al disclose of providing access upon validating the confidence score, but is silent in disclosing of having varying levels of security wherein providing access comprises determining a level of secured data that may be accessed by a user. It is disclosed by Fritch et al of authenticating a user and determining a clearance level of a user that may have a range of clearance levels which is determined by an access control list, or ACL (level of secured data), that dictates the user's rights (col. 1, lines 39-44; col. 6, lines 18-21; col. 7, lines 4-8; and col. 10, lines 8-11). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to have varying levels of access, which indicates appropriate permissions, or levels of secured data that may be accessed by a user. The teachings of Fritch et al recites motivation by disclosing that problems in the prior art exist wherein different servers can provide the same user with differing degrees of access to the same information and this can lead to allowing unauthorized access to sensitive information so the teachings of Fritch et al provide a consistent access policy in a network (col. 2, lines 10-15,26-29). It is obvious

that the teachings of Fritch et al would have allowed the teachings of Kanevsky et al in to provide a consistent access policy by allowing varying levels of access.

As per claims 2 and 13, Kanevsky et al discloses of confidence score is computed based on the identity claim using speech input from the user, wherein the confidence score is a measure of confidence in the validity of the identity claim (col. 3, lines 41-43). If the score matches a threshold value, the user is provided access to secured data based on the computed confidence score (col. 3, lines 44-48 and as recited in the abstract). In providing access by matching of the confidence score, it is interpreted by the examiner that the confidence score is maintained as the system state since that is the parameter submitted by the user for authentication and validation (col. 3, lines 44-48).

As per claims 3 and 14, Kanevsky et al does not teach further comprising the steps of partitioning the secured data into a plurality of data classes, assigning a security level to each of the data classes, and constructing an access map based on the security levels for accessing the secured data. Fritch teaches further comprising the steps of partitioning the secured data into a plurality of classification levels (data classes)(col. 1, line 50), assigning a security level to each of the data classes (col. 6, lines 34-37), and constructing an access map based on the security levels for accessing the secured data (col. 8, lines 28-30). Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky et al with the teachings of Fritch et al to include further comprising the steps of partitioning the secured data into a plurality of data classes, assigning a security level

to each of the data classes, and constructing an access map based on the security levels for accessing the secured data with the motivation to provide a consistent access policy in a computer network as is disclosed by Fritch et al (col. 2, lines 28-29).

As per claims 4 and 15, Kanevsky et al is relied upon for a confidence score is computed based on the identity claim using speech input from the user, wherein the confidence score is a measure of confidence in the validity of the identity claim (col. 3, lines 41-43). Kanevsky et al does not teach further comprising the steps of selecting a range of confidence scores, partitioning the range of user information into a plurality of regions, and assigning each region to one of the security levels. Fritch et al teaches further comprising the steps of selecting a range of user information (col. 2, lines 64), partitioning the user information into a clearance levels (plurality of regions)(col. 6, line 18-20), determining the access rights of the user with respect to a particular information object or class of information objects (assigning each region to one of the security levels)(col. 8, lines 28-30). Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky et al with the teachings of Fritch et al to include further comprising the steps of selecting a range of user information; partitioning the user information into a plurality of regions; and assigning each region to one of the security levels with the motivation to provide a consistent access policy in a computer network as is suggested by Fritch et al (col. 2, lines 28-29).

As per claims 5 and 16, Kanevsky et al is relied upon for a confidence score is computed based on the identity claim using speech input from the user, wherein the

confidence score is a measure of confidence in the validity of the identity claim (col. 3, lines 41-43). Kanevsky et al does not teach wherein the step of providing the user access to secured data determining a given region of the plurality of regions which comprises the user information, determining the security level assigned to the given region, and accessing secured data using the access map based on the security level assigned to the given region. Fritch et al teaches wherein the step of providing the user access to secured data comprises the steps of: determining a clearance level (a given region)(col. 6, line 18-20) of the plurality of regions associated to a user (col. 2, lines 64); determining the classification levels (security level)(col. 1, line 50) assigned to the given region; and accessing secured data using the access map based on the security level assigned to the given region (col. 8, lines 28-67). Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky with the teachings of Fritch to include wherein the step of providing the user access to secured data based on the user information comprises the steps of: determining a given region of the plurality of regions which comprises the user information; determining the security level assigned to the given region; and accessing secured data using the access map based on the security level assigned to the given region with the motivation to provide a consistent access policy in a computer network (Fritch, col. 2, lines 28-29).

As per claims 6 and 17, Kanevsky does not teach wherein the step of accessing secured data using the access map comprises the step of allowing access to secured data that is assigned to the security level of the given region and secured data assigned

to at least one security level that is lower than the security level of the given region. Fritch et al teaches wherein the step of accessing secured data using the access map comprises the step of allowing access to secured data that is assigned to the security level of the given region and secured data assigned to at least one security level that is lower than the security level of the given region (i.e. one suitable policy implements the familiar Bell-LaPadula model, which may be summarized by the rule "No read up" and "No write down." That is the task cannot read from information objects that are more sensitive, and cannot write to objects that are less sensitive, that the sensitivity level [effective clearance level(s)] of the task itself.) (col. 8, lines 40-45). Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky et al with the teachings of Fritch et al to include wherein the step of accessing secured data using the access map comprises the step of allowing access to secured data that is assigned to the security level of the given region and secured data assigned to at least one security level that is lower than the security level of the given region with the motivation to provide a consistent access policy in a computer network as suggested by Fritch et al (col. 2, lines 28-29).

As per claims 7,8,18, and 19, Kanevsky et al discloses of a confidence score is computed based on the identity claim using speech input from the user, wherein the confidence score is a measure of confidence in the validity of the identity claim (col. 3, lines 41-43). If the score matches a threshold value, the user is provided access to secured data based on the computed confidence score (col. 3, lines 44-48). The user requests (user query) access to a service and if the service is interrupted (occurrence of

a predetermined event), the user needs to be re-verified by recomputing the confidence score (col. 1, lines 23-25; col. 3, lines 44-48; and col. 12, lines 38-41).

As per claim 23, Kanevsky et al discloses of an apparatus (system) for incremental access authentication (col. 3, lines 12-20 and col. 12, lines 38-41). An identity claim is received from a user wherein the first spoken utterances of the speaker are received and the first spoken utterances (dialog session) containing indicia of the speaker (col. 3, lines 23-25). A confidence score is computed by the score estimator (computation module) based on the identity claim using speech input from the user, wherein the confidence score is a measure of confidence in the validity of the identity claim (col. 3, lines 41-43 and col. 6, lines 39-42). Kanevsky et al discloses that the computation may occur for as many iterations (periodic basis) as desired (col. 6, lines 61-65). If the score matches or exceeds a threshold value, the user is provided access to secured data based on the computed confidence score (col. 3, lines 44-48 and as recited in the abstract). The central server (dialog manager) controls access to the database (col. 1, lines 23-29 and col. 7, lines 15-25). Kanevsky et al does not teach further comprising the steps of partitioning the secured data into a plurality of data classes and assigning a security level to each of the data classes that limits accessing the secured data. Fritch teaches further comprising the steps of partitioning the secured data into a plurality of classification levels (data classes)(col. 1, line 50) and assigning a security level to each of the data classes that limits accessing secured data (col. 6, lines 34-37). Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky et al with the teachings

of Fritch et al to include further comprising the steps of partitioning the secured data into a plurality of data classes and assigning a security level to each of the data that limits access to the secured data with the motivation to provide a consistent access policy in a computer network as is disclosed by Fritch et al (col. 2, lines 28-29).

As per claim 24, Kanevsky et al is relied upon for a confidence score is computed based on the identity claim using speech input from the user, wherein the confidence score is a measure of confidence in the validity of the identity claim (col. 3, lines 41-43). The teachings of Kanevsky does not teach further comprising an access map for mapping each data class with the corresponding range of user access levels, wherein the access map is utilized by the dialog manager to provide access to data based on the last computed user access level. Fritch et al further discloses of an access map for mapping each data class with the corresponding user access levels, wherein the access map is utilized by the dialog manager to provide access to data based on the last computed user's access level (col. 8, lines 28-30). Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Kanevsky et al with the teachings of Fritch et al to include further comprising an access map for mapping each data class with the corresponding range of user access levels, wherein the access map is utilized by the dialog manager to provide access to data based on the last computed user access level with the motivation to provide a consistent access policy in a computer network as suggested by Fritch et al (col. 2, lines 28-29).

As per claim 25, Kanevsky et al discloses of confidence score is computed based on the identity claim using speech input from the user, wherein the confidence score is a measure of confidence in the validity of the identity claim (col. 3, lines 41-43). If the score matches a threshold value, the user is provided access to secured data based on the computed confidence score (col. 3, lines 44-48 and as recited in the abstract). In providing access by matching of the confidence score, it is interpreted by the examiner that the confidence score is maintained as the system state since that is the parameter submitted by the user for authentication and validation (col. 3, lines 44-48).

7. Claims 9-11,20-22, and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky et al, U.S. Patent 5,897,616 in view of Fritch et al, U.S. Patent 6,105,132 in further view of French et al, U.S. Patent 6,321,339.

As per claims 9,20, and 26, the teachings of Kanevsky et al are relied upon for comparision of a confidence score in regards to user's speech patterns. The combination of Kanevsky et al and Fritch et al fail to disclose of n the confidence score is based on a linear function of statistical models that characterize the score under a plurality of conditions. French et al teaches wherein the confidence score is based on a linear function of statistical models that characterize the score under a plurality of conditions (i.e. additionally, the checks of preprocessing step 26 may include the use of a credit card application fraud model, or some other model which statistically analyzes response data. For example, the data supplied by the user may be modeled and graded for confidence level based upon empirical models supplied by third party

vendors or available internally) (col. 11, lines 42-47). Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky with the teachings of French to include wherein the confidence score is based on a linear function of statistical models that characterize the score under a plurality of conditions with the motivation of enabling different levels of authentication to be performed based on the level of security desired, thus reducing costs and unnecessary use of system resources as suggested by French et al (col. 2, lines 62-65).

As per claims 10,21, and 27, Kanevsky teaches wherein the confidence score comprises one of (1) a first component for considering a single mode implementation and (2) the first component and a second component for considering a multi-modal implementation (i.e. it is further to be understood that P(acoustic data|speaker$_i$) may be computed using some acoustic models for speakers that may be represented as Hidden Markov Models (HMM)) (col. 11, lines 15-17). The Examiner interprets a Hidden Markov Model representation as a single mode implementation.

As per claims 11,22, and 28, Kanevsky teaches wherein the confidence score comprises a mixing factor for weighting the first and second component in a multi-modal implementation (i.e. in another embodiment, one can interpret P(speaker$_i$) as a weighted factor and update a general speaker score using a known formula) (col. 11, lines 18-20). The Examiner interprets the P(speaker$_i$) value to be equivalent to the confidence score.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Trandal et al, U.S. Patent 6,088,428 discloses a voice controlled messaging system and processing method.

Gressel, U.S. Patent 6,311,272 discloses a biometric system and techniques suitable therefor.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

2/5/05

CR

February 5, 2005